UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,887	04/05/2004	Do-heon Kim	Q79993	2675

23373 7590 07/09/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
LINDSEY, MATTHEW S	
ART UNIT	PAPER NUMBER
2151	

MAIL DATE	DELIVERY MODE
07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,887	KIM ET AL.	
	Examiner	Art Unit	
	MATTHEW S. LINDSEY	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8-10,13-19 and 22-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-10,13-19 and 22-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 April 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-6, 8-10, 13-19 and 22-26 are pending in this application. Claims 2, 7, 11-12 and 20-21 have been canceled as filed on 7 April 2008.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-5, 8-10, 13-19 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shah et al. (US 2003/0051009 A1), hereinafter Shah in view of Sherman et al. (US 5,075,884), hereinafter Sherman.

4. With respect to Claim 1, Shah disclosed: "A network connection apparatus (Abstract, lines 1-2; [0018], lines 1-4), comprising: a computer readable medium storing a computer program ([0048], lines 1-8), which when executed by a processor, comprises a join module for connecting a second network ([0018], lines 1-4), to which the join module belongs, with a first network in response to an inter-network connection request message transmitted from the first network ([0021], lines 1-6)",

"a connection module for receiving the inter-network connection request message transmitted from the first network and connecting the first network with the second network ([0024], lines 1-3)", and

"a transmission module for transmitting a requested network command message requested by the first network ([0025], lines 4-8)".

Shah did not explicitly state: "setting a security level of the first network to a set security level, and controlling network command messages in response to the set security level", "an authentication/security module for determining whether to allow a connection of the first network that has transmitted the inter-network connection request message to the connection module, and setting and checking the security level of the first network", "when the connection is allowed by the authentication/security module", or "wherein the security level is applied differently depending on the first network to be connected".

However, Sherman disclosed: "setting a security level of the first network to a set security level (Col. 4, lines 33-36, 60-62, where each port has a defined security level specified, or set, by a TCB, and a port can be used to communicate with other networks, hence specifying a security level of a port which communicates with another network sets the security level of the other network), and controlling network command messages in response to the set security level (Col. 4, lines 36-41, where communication occurs only between equivalent security levels)",

"an authentication/security module for determining whether to allow a connection of the first network that has transmitted the inter-network connection request message to the connection module (Col. 4, lines 49-52), and setting and checking (Col. 4, lines 36-41, where only nodes of equivalent security levels can communicate and therefore the security level must be checked) the security level of the first network (Col. 4, lines 60-62, where each port has a defined security level specified, or set, by a TCB, and a port can be used to communicate with other networks, hence specifying a security level of a port which communicates with another network sets the security level of the other network)",

"when the connection is allowed by the authentication/security module (Col. 4, lines 36-41, where nodes of equivalent security levels can communicate)", and

"wherein the security level is applied differently depending on the first network to be connected (Col. 4, line 64 – Col. 5, line 3, where each processor associated with a port processes data at a set level such as secret or top secret, and thus the security level is applied differently depending on the network to be connected)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communications of Shah with teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Therefore by combining the network

communications of Shah with the security system of Sherman, one can communicate with a home network from an external node without unauthorized disclosure of information.

5. With respect to Claim 3, the combination of Shah and Sherman disclosed: "The apparatus as claimed in claim 1, wherein the computer program stored on the computer-readable medium further comprises: a management module for collecting and managing information about devices present in the second network (Shah, [0031], lines 1-3) by performing a discovery process for the devices (Shah, [0031], lines 7-10); and a component module for generating a component representing services of the devices present in the second network on a basis of the information about the devices collected by the management module (Shah, [0031], lines 3-7)".

6. With respect to Claim 4, the combination of Shah and Sherman disclosed: "The apparatus as claimed in claim 3, wherein the computer program stored on the computer-readable medium further comprises: a stack module for transmitting a control message to the devices present in the second network (Shah, [0033], lines 1-3); and a lookup service module for storing information about the component generated by the component module in a lookup table (Shah, [0031], lines 1-5), and searching for component information of a specific device upon a request for a service of the specific device (Shah, [0031], lines 10-15)".

7. With respect to Claim 5, the combination of Shah and Sherman disclosed: "The apparatus as claimed in claim 1, wherein the connection module contains connection information about the first network or the devices present in the first network (Shah, [0031], lines 1-5)".

8. With respect to Claim 8, the combination of Shah and Sherman disclosed: "The apparatus as claimed in claim 1, wherein the transmission module transmits the network command messages transmitted and received between the first network and the second network to which the join module belongs (Shah, [0032], lines 4-11)".

9. With respect to Claim 9, Shah disclosed: "A method for connecting separate networks (Abstract, lines 1-5), comprising: (a) transmitting an initial inter-network connection request message to a second network by a first network ([0021], lines 1-5)", and "(c) transmitting a network command message to the second network by the first network ([0021], lines 3-6)".

Shah did not explicitly state: "(b) analyzing the initial inter-network connection request message and setting a security level of the first network to a set security level by the second network", "(d) searching, by the second network, the set security level of the first network which has transmitted the network command message to generate a searched security level; (e) transmitting the searched security level and the network command message to the second network; wherein the security level is applied differently depending on the first network to be connected; and wherein (b) comprises

analyzing the initial inter-network connection request message and determining whether to allow a connection between the first and the second networks".

However, Sherman disclosed: "(b) analyzing the initial inter-network connection request message and setting a security level of the first network to a set security level by the second network (Col. 4, lines 60-61)" and "(d) searching, by the second network, the set security level of the first network which has transmitted the network command message to generate a searched security level (Col. 4, lines 49-52, the guard means ensures correct security levels and manages communication); (e) transmitting the searched security level and the network command message to the second network (Col. 4, lines 49-52); wherein the security level is applied differently depending on the first network to be connected (Col. 4, line 64 – Col. 5, line 3, where each processor associated with a port processes data at a set level such as secret or top secret, and thus the security level is applied differently depending on the network to be connected); and wherein (b) comprises analyzing the initial inter-network connection request message and determining whether to allow a connection between the first and the second networks (Col. 4, lines 49-52)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce

necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows controlling access to the devices on a home network to an external network.

10. With respect to Claim 18, Shah disclosed: "A method for connecting separate networks (Abstract, lines 1-5; [0018], lines 1-4), comprising: (a) receiving an initial inter-network connection request message from an external network ([0021], lines 1-5)", and "(c) receiving a network command message from the external network ([0021], lines 3-6)".

Shah did not explicitly state: "(b) analyzing the initial inter-network connection request message and setting a security level of the external network to a set security level" or "(d) searching the set security level of the external network which has transmitted the network command message to generate a searched security level; (e) transmitting the searched security level and the network command message to another network to which the external network is connected; wherein the security level is applied differently depending on the external network to be connected; and wherein (b) comprises analyzing the initial inter-network connection request message and determining whether to allow a connection between the external and the another networks".

However, Sherman disclosed: "(b) analyzing the initial inter-network connection request message and setting a security level of the external network to a set security level (Col. 4, lines 60-61)" and "(d) searching the set security level of the external

network which has transmitted the network command message to generate a searched security level (Col. 4, lines 49-52, the guard means ensures correct security levels and manages communication); (e) transmitting the searched security level and the network command message to another network to which the external network is connected (Col. 4, lines 49-52); wherein the security level is applied differently depending on the external network to be connected (Col. 4, line 64 – Col. 5, line 3, where each processor associated with a port processes data at a set level such as secret or top secret, and thus the security level is applied differently depending on the network to be connected); and wherein (b) comprises analyzing the initial inter-network connection request message and determining whether to allow a connection between the external and the another networks (Col. 4, lines 49-52)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system of Shah with the teachings of Sherman to include a security system. Motivation to combine these references comes from Sherman to "prevent unauthorized disclosure of information" (Col. 3, lines 31-32) and from Shah where it is disclosed that "the area server 210 may also enforce necessary security measures to make sure that the communication with the external node 110 is secure" ([0023], second col., lines 2-4). Combining these references allows controlling access to the devices on a home network to an external network.

11. With respect to Claims 10 and 19, the combination of Shah and Sherman disclosed: "wherein the initial inter- network connection request message includes

information about the first network that has transmitted the initial inter-network connection request message (Shah, [0004], lines 7-12, using TCP/IP includes sending data packets that contain headers with information about the source, in this case the header would contain information about the external network)".

12. With respect to Claims 13 and 22, the combination of Shah and Sherman disclosed: "wherein (e) comprises transmitting a notify message to the first network (Shah, [0038], lines 4-11)".

13. With respect to Claims 14 and 23, the combination of Shah and Sherman disclosed: "further comprising: transmitting a response message for the network command message by the second network (Shah, [0026], lines 6-8) and checking a security level for the response message of the second network (Sherman, Col. 4, lines 42-49, security levels must be checked to control the flow of information where different levels of security are present and only equivalent security levels can communicate)".

14. With respect to Claims 15 and 24, the combination of Shah and Sherman disclosed: "further comprising, if the network command message is a search message for looking for a device present in the second network (Shah, [0036], lines 5-7), searching for devices corresponding to the searched security level of the first network (Sherman, Col. 4, lines 42-49) and transmitting information about the devices (Shah, [0037], lines 5-10)".

15. With respect to Claims 16 and 25, the combination of Shah and Sherman disclosed: "further comprising, if the network command message is a message for requesting information about a specific device present in the second network (Shah, [0026], lines 3-6), searching component information about the specific device among component information about the devices present in the second network (Shah, [0031], lines 1-10) and transmitting the component information about the specific device (Shah, [0037], lines 5-10)".

16. Claims 6, 17, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shah and Sherman, and further in view of Zintel et al. (US 6,725,281).

17. With respect to Claim 6, the combination of Shah and Sherman did not explicitly state: "wherein the connection module checks periodically whether the first network transmits a transmitted network command message every predetermined period of time, and terminates the connection if the transmitted network command message is not received within the predetermined period of time".

However, Zintel disclosed: "The apparatus as claimed in claim 2, wherein the connection module checks periodically whether the first network transmits a transmitted network command message every predetermined period of time (Col. 36, lines 13-14),

and terminates the connection if the transmitted network command message is not received within the predetermined period of time (Col. 36, lines 13-15)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system and security protocol of Shah and Sherman with the teachings of Zintel to include terminating connection if a message is not received in a certain period of time. Motivation to combine these references comes from Zintel, "The scenario is this: A UCP subscribes to a CD, then the UCP reboots. Meanwhile, the CD is still trying to send notifications to that UCP. If the UCP never comes back, the subscription would be leaked because the UCP never told the CD that it was going away." (Col. 36, lines 3-8). By combining the network communication and security system of Shah and Sherman with the timeout feature of Zintel, the network communications will be protected against leaked subscriptions.

18. With respect to Claims 17 and 26, the combination of Shah and Sherman did not explicitly state: "further comprising, if the network command message is not received from the first network within a predetermined period of time, terminating a connection between the first and the second networks".

However Zintel disclosed: "further comprising, if the network command message is not received from the first network within a predetermined period of time (Col. 36, lines 13-14), terminating a connection between the first and the second networks (Col. 36, lines 13-15)".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the network communication system and security protocol of Shah and Sherman with the teachings of Zintel to include terminating connection if a message is not received in a certain period of time. Motivation to combine these references comes from Zintel, "The scenario is this: A UCP subscribes to a CD, then the UCP reboots. Meanwhile, the CD is still trying to send notifications to that UCP. If the UCP never comes back, the subscription would be leaked because the UCP never told the CD that it was going away." (Col. 36, lines 3-8). By combining the network communication and security system of Shah and Sherman with the timeout feature of Zintel, the network communications will be protected against leaked subscriptions.

Response to Arguments

19. Regarding applicant's remarks, see pg 11, I. Formal Matters, filed 7 April 2008, with respect to information disclosure statements dated 13 September 2006, 10 August 2005, 16 May 2005, 10 September 2004 and 12 August 2004. Examiner spoke to Peter McKenna, Registration No. 38551, over the telephone on 1 July 2008 and confirmed all Information Disclosure statements are signed and appear in the Image File Wrapper.

20. Applicant's arguments, see pg 11, II. Drawing Objection, filed 7 April 2008, with respect to Drawing objections have been fully considered and are persuasive. The Objection of the drawings has been withdrawn.

21. Applicant's arguments, see pg 12, III. Claim Rejection under 35 USC 101, filed 7 April 2008, with respect to 35 USC 101 rejection of claims 1-8 have been fully considered and are persuasive. The rejection of claims 1-8 under 35 USC 101 has been withdrawn.

22. Applicant's arguments, see pg 12, IV. Claim Rejection under 35 USC 103(a), filed 7 April 2008 have been fully considered but they are not persuasive. Applicant argues: "Sherman fails to teach or suggest the claimed features of setting the security level for the first network, and applying a different security level according to the network that transmits the connection-request message between networks" (pg 14, lines 1-3).

Examiner respectfully disagrees. Sherman disclosed: "In accordance with the invention, **each port of the workstation 12 has a defined security level as specified by a TCB** (*where a port can be used to communicate with other networks, hence specifying a security level of a port which communicates with another network sets the security level of the other network*), and a processor 42, 44 is associated with each TCB 20, 22 and coupled thereto via a dedicated port 14, 16, respectively. **Each processor 42, 44 associated with a port 14, 16 is restricted to processing data at the security level associated with the defined security level of the TCB** 20, 22. For example, the first processor 42 may be a processor dedicated to process functions classified as "Secret" while the second processor 44 may be a processor dedicated to process functions classified as "Top Secret." (*where each processor associated with a port*

processes data at a set level such as secret or top secret, and a port can be used to communicate with other networks, and thus the security level is applied differently depending which network to be connected, a top secret network would communicate with a top secret port and a secret network would communicate with a secret port)" (Col. 4, line 60 – Col. 5, line 3, emphasis added).

Applicant further argues: "However, Sherman does not teach or suggest "setting a security level" " (pg 14, lines 12-13). Examiner respectfully disagrees. Sherman disclosed: "In accordance with the invention, each **port of the workstation 12 has a defined security level as specified by a TCB**" (Col. 4, lines 60-62, emphasis added).

23. Applicant's arguments, see pg 14, B. Claims 2-5, 7 and 8, filed 7 April 2008 have been fully considered but they are not persuasive. Applicant argues the dependency of claims 3-5 and 8 on independent claim 1 make them patentable. See rejection and arguments above with respect to claim 1.

24. Applicant's arguments, see pg 15, C. Claims 9-16, filed 7 April 2008 have been fully considered but they are not persuasive. Applicant argues claim 9 is patentable because of similar reasons as claim 1. Applicant also argues that because claims 13-16 are dependent on claim 9, they are patentable. See rejection and arguments above with respect to claim 1.

25. Applicant's arguments, see pg 15, D. Claims 18-25, filed 7 April 2008 have been fully considered but they are not persuasive. Applicant argues claim 18 is patentable because of similar reasons as claim 1. Applicant also argues that because claims 22-25 are dependent on claim 18, they are patentable. See rejection and arguments above with respect to claim 1.

26. Applicant's arguments, see pg 15, V. Claim Rejection under 35 USC 103(a) over Shah in view of Sherman, in further view of Zintel, filed 7 April 2008 have been fully considered but they are not persuasive. Applicant argues the dependency of claims 6, 17 and 26 on independent claims 1, 9 and 18 make them patentable. See rejection and arguments above with respect to claims 1, 9 and 18.

Conclusion

27. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW S. LINDSEY whose telephone number is (571)270-3811. The examiner can normally be reached on Mon-Thurs 7:30-5, Fridays 7:30-1.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MSL
7/1/2008

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151